Method for storing and operating sensitive information in security module, and associated security module

Patent number:	CN1222991
Publication date:	1999-07-14
Inventor:	HAZARD MICHEL (FR)
Applicant:	BULL CP8 (FR)
Classification:	
- international:	G07F7/10; H04L9/08
- european:	
Application number:	CN19980800480 19980312
Priority number(s):	FR19970002973 19970313

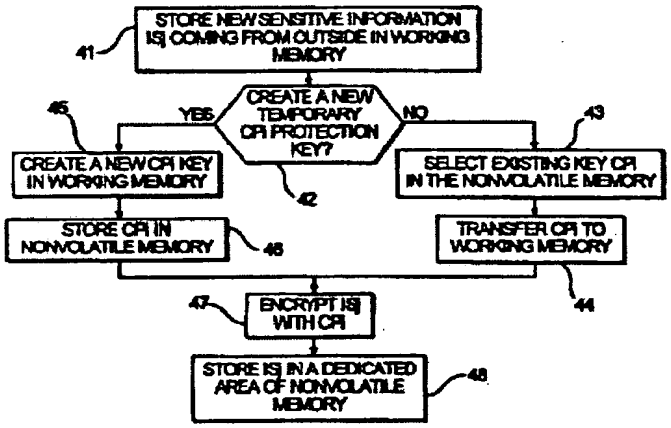
Also published as:

WO9840853 (A1)
EP0914640 (A1)
US6658566 (B1)
FR2760871 (A1)
EP0914640 (B1)

more >>

Abstract not available for CN1222991
Abstract of corresponding document: **US6658566**

The invention relates to a process for storing and using sensitive information in a security module and to a security module arranged to implement the process, and protect the sensitive information against fraudulent utilization. The sensitive information ISj is stored in a form {overscore (ISj encrypted using a temporary encrypting protection key CPi, whose content varies over time. The sensitive information {overscore (ISj is decrypted before being used in a given operation, using a temporary decrypting protection key CPid. Before the contents of the encrypting and decrypting keys are varied, the sensitive information {overscore (ISj is decrypted with the current decrypting key, and then it is re-encrypted with the new encryption key to obtain a new encrypted form, different from the previous one.



[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
G07F 7/10
H04L 9/08

[12]发明专利申请公开说明书

[21]申请号 98800480.1

[43]公开日 1999年7月14日

[11]公开号 CN 1222991A

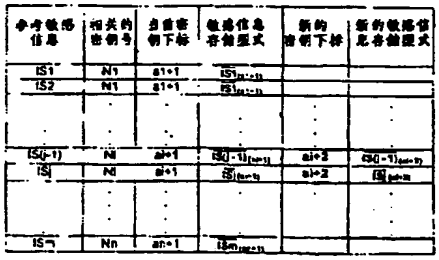
[22]申请日 98.3.12 [21]申请号 98800480.1
[30]优先权
[32]97.3.13 [33]FR [31]97/02973
[86]国际申请 PCT/FR98/00503 98.3.12
[87]国际公布 WO98/40853 法 98.9.17
[85]进入国家阶段日期 98.12.14
[71]申请人 布尔CP8公司
地址 法国卢维西恩尼斯
[72]发明人 米歇尔·哈泽德
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 马 浩

权利要求书4页 说明书10页 附图页数5页

[54]发明名称 用于在保密模块中存储和使用敏感信息的方法及相关的保密模块

[57]摘要

本发明涉及一种在保密模块中存储和使用敏感信息的方法和一种用于实现这种方法从而保护敏感信息不被非法使用的保密模块。按照本发明，敏感信息ISj使用其内容随时间而改变的一个暂时加密保护密钥CPi以加密的形式$\overline{ISj}$被存储。敏感信息$\overline{ISj}$在给定的处理中被使用之前利用暂时解密保护密钥CPid解密。在改变加密和解密密钥的内容之前，敏感信息$\overline{ISj}$利用当前解密密钥被解密，然后用新的加密密钥再加密，从而获得和原来不同的新的加密形式。



ISSN1008-4274

权 利 要 求 书

1.一种用于在一个保密模块（ 8 ）中存储敏感信息 ISj 的方法，所述保密模块包括信息处理装置（ 9 ）和信息存储装置（ 10， 14 ），其特征在于，所述方法包括以下步骤:

由保密模块使用由保密模块提供的当前型式 CPi（ai+1）中的暂时加密保护密钥 CPi 和在所述存储装置中和相关的一个解密算法一道存储的一个加密算法加密敏感信息 ISj；

使保密模块在该模块的一个非易失存储器（ 10 ）中存储与识别数据相关的敏感的加密信息 $\overline{ISj}$（ai+1），所述识别数据限定具有和所述暂时加密保护密钥 CPi 的所述当前型式 CPi（ai+1）相关的一个当前型式 CPid（ai+1）的一个暂时解密保护密钥 CPid，所述识别数据包括一个密钥标识 CPid 和在几种型式当中确定所述解密密钥的当前型式 CPid（ai+1）的一个更新下标（ ai+1 ）；以及

如果其当前型式为 CPid（ai+1）的暂时解密保护密钥 CPid 未被存储在所述非易失存储器（ 10 ）中，则使保密模块存储这一型式.

2.如权利要求 1 所述的存储方法，其中保密模块包括产生随机数的装置，用于提供一个随机数的连续的不同的型式，而由保密模块提供的暂时加密保护密钥 CPi 的每种型式从所述随机数的不同型式中获得.

3.一种用于分析在一个保密模块（ 8 ）中的敏感信息 ISj 的方法，所述保密模块包括信息处理装置（ 9 ）和信息存储装置（ 10， 14 ），其中敏感信息 ISj 通过保密模块使用具有由保密模块提供的当前型式 CPi（ai+1）的一个暂时加密保护密钥 CPi 和在所述存储装置中与相关的解密算法一道存储的一个加密算法被转换为加密形式，同时具有加密形式 $\overline{ISj}_{(ai-1)}$ 的敏感信息和识别数据一道被存储在保密模块的一个非易失存储器（ 10 ）中，所述识别数据限定一个具有与暂时加密保护密钥 CPi 的所述一个当前型式 CPi（ai+1）相关的当前型式 CPid（ai+1）的暂时解密保护密钥 CPid，所述识别数据包括一个密钥标识 CPid 和在几种型式当中确定所述解密密钥的所述当前型式 CPid（ai+1）的一个更新下标（ ai+1 ），其特征在于包括以下步骤:

使保密模块利用所述识别数据在来自模块内部或外部的一个请求使用敏感信息 ISj 期间选择与该敏感信息相关的所述暂时解密保护密钥 CPid 的所述当前型式 CPid（ai+1）；

使保密模块利用暂时解密保护密钥 CPid 的当前型式 CPid（ai+1）和解密算法解密加密的敏感信息 $\overline{ISj}_{(ai+1)}$，并暂时存储这样获得的解密形式的敏感信息 ISj，使得该敏感信息使用之后其从保密模块中消失；以及

使保密模块使用解密形式的敏感信息 ISj。

4.如权利要求 3 所述的操作方法，为了定期地修改敏感信息的加密形式，包括以下步骤：

使保密模块使用和其相关的暂时解密保护密钥 CPid 的当前型式 CPid（ai+1）以及所述解密算法解密以当前型式 $\overline{ISj}_{(ai+1)}$ 存储的敏感信息；

使保密模块选择暂时加密保护密钥 CPi 的一个新的型式 CPi（ai+2）；然后，

使保密模块利用暂时加密保护密钥的新的型式 CPi（ai+2）和所述加密算法再加密解密的敏感信息 ISj，从而产生敏感信息的一个新的加密形式 $\overline{ISj}_{(ai+2)}$；以及

在保密模块中存储具有新的加密形式 $\overline{ISj}_{(ai+2)}$ 的敏感信息和与暂时加密保护密钥的所述新的型式 $CPi_{(ai+2)}$ 相关的暂时解密保护密钥 CPid 的一个新的型式 CPid（ai+2）。

5.如权利要求 4 所述的操作方法，其中保密模块包括产生随机数的装置，用于提供随机数的不同的连续的型式，借以使由保密模块提供的暂时加密保护密钥 CPi 的每种当前型式 CPi（ai+1）和新的型式 CPid（ai+2）从所述随机数的各个不同型式中获得。

6.如权利要求 4 所述的操作方法，其中每个暂时解密保护密钥的两个最近的型式，即倒数第二个型式 $CPid_{ai}$ 和最后的一个型式 CPid（ai+1），被存储在保密模块的非易失存储器（10）中，并且，当任何暂时加密保护密钥的一个新的型式 CPi（ai+2）由保密模块产生时，在非易失存储器（10）中存储一个新的与暂时解密保护密钥 CPid 相关的相应型式 CPid（ai+2）代替倒数第二个型式 $CPid_{ai}$。

7.如权利要求6所述的操作方法，其中敏感信息IS（j-1）和ISj的若干项利用和同一个暂时加密保护密钥CPi不同的一个倒数第二个型式CPi_{ai}和一个最后的型式CPi（ai+1）分别被加密，从而给出加密的形式$\overline{IS(j-1)}_{ai}$和$\overline{ISj}_{(ai+1)}$，并且，当所述敏感信息的一个新的型式必须由保密模块产生时，执行以下的步骤:

使保密模块使用和其相关的暂时加密保护密钥 CPid 的倒数第二个$CPid_{ai}$解密由暂时加密保护密钥CPi的倒数第二个型式CPi_{ai}加密的敏感信息$\overline{IS(j-1)}_{ai}$;

使保密模块利用暂时加密保护密钥的所述最后型式CPi（ai+1）再加密解密的敏感信息 IS(j-1)，从而产生敏感信息的一个新的加密形式$\overline{IS(j-1)}_{(ai+1)}$；以及

在保密模块中存储具有其新的加密形式$\overline{IS(j-1)}_{(ai+1)}$的这个敏感信息;

并且，为了产生敏感信息IS（j-1），ISj 的所述新的型式，执行以下步骤:

使保密模块利用和暂时加密保护密钥CPi的所述最后型式CPi（ai+1）相关的暂时解密保护密钥CPid的一个最后型式CPid（ai+1）解密与所述暂时加密保护密钥CPi相关的所有敏感信息$\overline{IS(j-1)}_{(ai+1)}$和$\overline{ISj}_{(ai+1)}$;

使保密模块利用暂时加密保护密钥的一个新的型式CPi（ai+2）和所述加密算法再加密解密的敏感信息IS（j-1），ISj，从而产生这一敏感信息的一个新的加密形式$\overline{IS(j-1)}_{(ai+2)}$和$\overline{ISj}_{(ai+2)}$；以及

在保密模块中存储具有其新的加密形式$\overline{IS(j-1)}_{(ai+2)}$和$\overline{ISj}_{(ai+2)}$的敏感信息和与暂时加密保护密钥的所述新的型式$CPi_{(ai+2)}$相关的暂时解密保护密钥CPid的一个新的型式CPid（ai+2）.

8.一种保密模块（8），包括处理信息的装置（9）和存储信息的装置（10，14），其特征在于还包括:

产生密钥的装置，其被如此设置，使得产生一个或几个暂时加密保护密钥 CP1,...,CPi,...,CPn 和相等数量的相关的暂时解密保护密钥CP1d,...,CPid,...,CPnd，并且，对于每个暂时加密保护密钥CPi和暂时解

密保护密钥 CPid，产生多个连续型式 CPi_{ai},CPi（ai+1）,CPi（ai+2）和 $CPid_{ai}$,CPid（ai+1）,CPid（ai+2）；

被设置用于使一个特定的暂时加密保护密钥 CPi 和一个与暂时加密保护密钥 CPi 相关的暂时解密保护密钥 CPid 与一个特定的敏感信息 ISj 相关联的装置；

加密装置，被设置用于利用与该敏感信息相关的暂时加密保护密钥的一个或另外的连续型式 CPi_{ai},CPi（ai+1）,CPi（ai+2）和存储在存储装置（10，14）中的一个加密算法对敏感信息 ISj 进行连续加密；以及

解密装置，被设置用于对于每个解密操作，利用所述暂时解密保护密钥的连续型式 $CPid_{ai}$,CPid（ai+1）,CPid（ai+2）当中的与用于进行相应加密的暂时加密保护密钥的型式相关的一个和存储在存储装置（10，14）中的一个解密算法，对敏感信息 Isj 进行连续解密.

9.如权利要求 8 所述的保密模块，包括产生随机数的装置，用于提供一个随机数的连续的和不同的型式，由保密模块提供的每个暂时加密保护密钥 CPi 的所述每个连续型式 CPi_{ai},CPi（ai+1）,CPi（ai+2）从所述随机数的各个不同型式中获得.

说　明　书

用于在保密模块中存储和使用敏感信息的方法及相关的保密模块

本发明涉及用于在保密模块中存储和使用敏感信息的方法及相关的保密模块.

“敏感信息”首先指的是对在保密模块中执行的操作的保密具有重大影响的任何信息，例如:

和用于对信息进行加密或解密操作的算法结合而使用的密钥，数据或个人鉴别或信息特征标记;

由用户在和保密模块联合操作的一个终端上提供的鉴别码（例如 PIN 个人识别码）;

经过扩展，术语“敏感信息”还指持有该信息的人认为是机密的信息，例如银行帐号，一个消息，或者甚至于一个完整的文件.

术语“保密模块”必须按照其一般意义理解，借以指一种这样的装置，这种装置的业务，在通信或信息网络中，要由管理网络的组织保持着，并在保护的情况下存储网络的保密和基本参数，例如密钥，或者更简单地指分配给网络用户的一种装置，其能够使每个用户访问网络，其中可能含有保密参数. 保密模块可以是一种包括计算机芯片的便携装置，例如银行信用卡.

本发明是基于以下的观察作出的，即，每个人都可以使用硬件设备，当在保密模块中的微型电缆逻辑装置中的程序或指令被执行时，想要作弊的人可以看到保密模块的电流消耗，尤其是如果使用 CMOS 技术的话. 更具体地说，可以识别读取 EEPROM 中的信息的程序的特定位置，尤其是上述定义的敏感信息.

因此,本发明的目的在于,通过特别是在敏感信息在EEPROM和RAM之间转移时，输入敏感信息的保护，或者反之亦然，利用暂时保护密钥对其加密，其中保护密钥的内容按照给定的频率改变，特别是按照和敏感信息的机密程度相关的频率而改变，来加强保密模块的安全性.

为此目的，本发明提供一种用于在保密模块中存储敏感信息 ISj 的方法，所述保密模块包括处理信息的装置和存储信息的装置，其特征在于，所述方法包括以下步骤:

由保密模块使用由保密模块提供的当前型式 CPi（ai+1）中的暂时加密保护密钥 CPi 和在所述存储装置中和相关的解密算法一道存储的加密算法加密敏感信息 ISj；

使保密模块在其非易失存储器中存储与识别数据相关的加密形式 $\overline{ISj}$（ai+1）的敏感信息，以定义一个以与暂时加密保护密钥 CPi 的所述当前型式 CPi（ai+1）相关的一个当前型式(version) CPid（ai+1）的暂时解密保护密钥 CPid，所述识别数据包括一个密钥标识 CPid 和在几种型式当中确定所述解密密钥的当前型式 CPid（ai+1）的一个更新下标（ai+1）；以及

如果以其当前型式 CPid（ai+1）的暂时解密保护密钥 CPid 未被存储在所述非易失存储器中，则由保密模块存储这种型式。

本发明还涉及一种使用保密模块中的敏感信息 ISj 的方法，所述保密模块包括处理信息的装置和存储信息的装置，其中敏感信息 ISj 通过保密模块使用由保密模块提供的当前型式 CPi（ai+1）的暂时加密保护密钥 CPi 和在所述存储装置中和相关的解密算法一道存储的加密算法被转换为加密形式，同时加密形式 $\overline{ISj}_{(ai+1)}$ 的敏感信息和识别数据一道被存储在保密模块的非易失存储器中，所述识别数据限定和暂时加密保护密钥 CPi 的所述当前型式 CPi（ai+1）相关的当前型式 CPid（ai+1）的暂时解密保护密钥 CPid，所述识别数据包括密钥标识 CPid 和在几种型式当中确定所述解密密钥的当前型式 CPid（ai+1）的更新下标（ai+1），其特征在于包括以下步骤:

使保密模块利用所述识别数据根据来自模块内部或外部的使用敏感信息 ISj 的每个请求选择和该敏感信息相关的所述暂时解密保护密钥 CPid 的所述当前型式 CPid（ai+1）；

使保密模块利用暂时解密保护密钥 CPid 的当前型式 CPid（ai+1）和解密算法解密加密的敏感信息 $\overline{ISj}_{(ai+1)}$，并暂时存储这样获得的解密形式的敏感信息 ISj，使得其在使用这一敏感信息之后从保密模块中消失；以及

使保密模块使用解密形式的敏感信息 ISj。

最后，本发明涉及一种执行上述步骤的保密模块.

本发明的其它细节和优点在参照附图对最佳的而非限制性的实施例说明之后将会更加清楚，其中:

图 1 是和数据处理装置一道操作的应用本发明的保密模块的图;

图 2 是表示一组暂时保护密钥及其各种属性的表;

图 3 是分别表示所有的敏感信息和暂时保护密钥属性的表;

图 4 是任意敏感信息 ISj 的初始加密程序的流程图;

图 5 是为了使用而进行处理的敏感信息解密程序 $\overline{ISj}$ 的流程图;

图 6 是任何暂时保护密钥 CPi 的定期刷新程序的流程图;

图 7 和图 8 是分别对应于图 2 和图 3 的表，只是其中包括暂时保护密钥或刷新的敏感信息; 以及

图 9 是任何敏感信息的定期刷新程序的流程图.

在给出的实施例中，图 1 所示的数据处理装置 1 包括微处理器 2，和其相连的有一个存储器 ROM 3，一个存储器 RAM 4，与保密模块 8 有或没有物理连接的协作装置 5 以及使数据处理装置可以和另一个类似的装置直接地或通过通信网络进行通信的发送接口 7.

此外，装置 1 可以具有存储装置例如软盘或者可换或不可换磁盘，输入装置（例如键盘和/或指定装置例如鼠标）和图 1 没有示出的显示装置.

数据处理装置可以包括安装在个人或公共处所的任何计算机设备，并且能够提供管理信息的装置或提供某种商品或服务的装置，该设备以固定的方式或便携的方式被安装. 这也可以涉及电信设备.

此外，保密模块 8 包括处理信息的装置 9，非易失存储器 10，易失的工作存储器 RAM14 和与数据处理装置协同工作的装置 13. 建立该模块为了在存储器 10 内限定一个保密区 11，一旦在保密区中记录信息，便从模块外部不能访问该信息，而只有使用处理装置 9 才能访问，以及自由区 12，其可由模块外部访问，用于读和/或写信息. 每个非易失存储器 10 的区域可以包括一个不能修改区 ROM 和一个可以修改区 EPROM， EEPROM 或包括快速式随机存取存储器 RAM，即，其具有 EEPROM 的特性，此外，还具有和一般 RAM 相同的存取时间.

作为保密模块 8，尤其可以使用具有可自编程的非易失存储器的微处

理器，如本申请人的美国专利 No. 4382279 中所述．如其第 1 栏第 13 － 25 行所述，该存储器的可自编程的特性相当于对于将该存储器中的程序 fi，它能够修改也位于该存储器中的另一个程序 fj 为程序 gj．虽然要被实现以便进行自编程的装置可以按照在设计处理信息的装置 9 时使用的技术而改变，但是应该记住，如果这种处理装置包括与非易失存储器相共的微处理器，并且按照前述的专利，这种装置可以包括:

和该存储器相关的数据和地址缓冲存储器;

用于在其中加载的存储器中进行写操作的程序，所述程序含有更具体的指令，用于在足够长的时间内，一方面维持存储器编程电压，另一方面维持要被写的数据及其地址，然而，同时这个写程序可以由逻辑电路写逻辑控制器代替．

在另一个实施例中，保密模块 8 的微处理器可以被位于一个半导体芯片中的逻辑电路代替，或者至少由所述逻辑电路实现．这种电路使用有线的非微编程的电子电路适用于进行计算，尤其是进行鉴别和特征标识．具体地说，它们可以是 ASIC（ Application Specific Integrated Circuit 专用集成电路）型的，例如参考 SLE 4436 商品生产的 SIEMENS 的元件，或者参考 ST 1335 由 SGS － THOMSON 生产的电子元件．

在一个优选的实施例中，保密模块 8 可以单片形式被设计在一个单独的芯片上．

作为上述的可自编程的非易失存储器微处理器的一种替代方案，保密模块的保密特性可以从使其位于防止捣毁的外壳中得到．

本发明使用几种暂时加密保护密钥 CP1,...CPi,...CPn 和几种相关的暂时解密保护密钥 CPd1，...CPdi,...CPdn．根据所使用的加密算法的类型，暂时解密保护密钥和暂时加密保护密钥可以相同或不同．这样，作为加密算法，我们一般使用对称密钥算法例如 DES（ Data Encryption Standard 数据加密标准）算法，借以使密钥对应于暂时加密保护密钥 CP1，...CPi,...CPn 中的一个．对于这种类型的算法，将使用和加密算法相反的解密算法，并且对于加密和解密，密钥将被不加区别地使用．换句话说，解密操作将使用和加密密钥相同的解密密钥．

在一个次优选的实施例中，使用公共密钥不对称算法例如 RSA 算法（发

明人 Rivest,Shamir 和 Adleman 发明的），它使用一个公共加密密钥和与加密密钥不同的另一个解密密钥．在这种情况下，保密模块存储两个密钥或参数，使用两种连续的型式对其重构．

在下面的附图说明中，这样使用具有密钥的对称算法，使得暂时解密保护密钥 CPd1，...CPdi,...CPdn 和暂时加密保护密钥 CP1，...CPi,...CPn 混同起来；为此，不再使用表示 CPd1，...CPdi,...CPdn，而代之以 CP1，...CPi,...CPn，因而被简单地称为“暂时保护密钥”而不规定它们是处理加密还是解密．

加密算法可以和用于与保密模块的应用有关的不同的功能的算法相同，或者可以是对于暂时密钥保护加密任务特定的或专用的加密算法．

图 2 的表包括开始栏，其中限定 n 个暂时保护密钥 CP1，...CPi,...CPn，它们分别具有用于对其进行标识的密钥号 N1，...Ni,...Nn．为了防止在保密模块的不适时的处理中发生任何中断，并且按照下面的所规定的，对于每个暂时保护密钥存储该密钥的两个连续的值，其每个由和该密钥相关的更新下标 a1,...ai,...an 标识．给予这更新下标一个更新的列．这样，密钥 CPi 具有由在时间上刚刚在其之前并由更新下标（ ai ）限定的值 CPi_{ai} 和由一个更新下标（ ai+1 ）确定的一个当前值 $CPi_{(ai+1)}$．不同的更新下标相互独立地改变．

在图 3 的表中的第一栏是 m 个敏感信息 IS1， IS2，...IS（ j-1 ）,ISj,...ISm 的号数，利用加密算法和从图 2 的表中选择的暂时保护密钥以加密的形式将其每个存储在保密模块中．在表的第二栏规定了用于每个敏感信息项的暂时保护密钥的号数．这样，暂时保护密钥 CP1（其号数是 N1 ）用于保护敏感信息 IS1， IS2，暂时保护密钥 CPi 保护敏感信息 IS（ j-1 ）,ISj,暂时保护密钥 CPn 只保护敏感信息 ISm．表中第三栏表示当暂时保护密钥用于加密敏感信息时的更新下标．这样，敏感信息 IS1，IS2，...ISj,...ISm 利用具有最新的更新下标（ a1+1),（ ai+1)或（ an+1 ）作为可应用的下标的密钥进行加密，而敏感信息 IS（ j-1 ）利用在最近的更新下标（ ai+1 ）之前的更新下标（ ai ）的密钥加密．表中的第四栏即最后一栏表示敏感信息的存储型式．因而，敏感信息 ISj 以加密的 $\overline{ISj}_{(ai-1)}$ 存

储，其相对于相关的暂时保护密钥具有更新下标（ ai+1 ）.

一般地说，图 2 和图 3 的表中包含的数据被存储在保密模块的非易失存储器 10 中，暂时保护密钥例如 CPi_{ai} 被存储在保密区 11 中，而其它的数据可以存储在保密区 11 或自由区 12 中. 关于这数据的大小，用位数表示时，密钥的位数，不论是暂时保护密钥 CPi 还是作为敏感信息 ISj 的密钥一般都是 64 位，而号数 Ni 和更新下标（ ai ）的位数一般为一比特. 注意图 2 的表中的第一栏可以不存储在保密模块中，然而，如果将这些暂时保护密钥存储在含有另一种类型的信息的区中，在确定相关信息的类型时将是有用的.

每个暂时保护密钥例如 CPi 具有由保密模块在内部产生的并随时间而改变的值. 在最佳实施例中，每个 CPi 密钥是一个随机数或由保密模块产生的随机数的函数，使得其随着时间而进行的变化是不能预测的. 这个随机数可以由软件产生，例如按照美国专利 5177790 号或 5365466 号中所述的方法或利用产生一个随机的物理大小的电路. 在一个次优选的实施例中，每个 CPi 密钥表示按照预定规则随时间而改变的数据. 例如，该数据等于被按 1 个单位规则增加的计数器的内容. 根据这种情况，每个暂时保护密钥 CPi 将或者被事先产生，或者在用于对敏感信息 ISj 加密时产生. 在所有情况下，暂时保护密钥 CPi 的产生以及敏感信息 ISj 的加密或解密将完全在保密模块的控制下进行，或者，在一些情况下，在特别可靠的从事保密模块工作的管理机构的控制下进行，此时只有保密模块或者所述的管理机构可以决定进行对没有权利的外部世界（即和保密模块协同工作的任何终端或普通用户）是透明的操作，即使这种操作可以由来自所述没有权利的外部世界的请求间接地控制，例如使敏感信息 ISj 输入密码计算例如信息的加密或标记或者一个信息或个人的鉴别中.

最通常的情况是，保密模块和没有权利的终端协同工作，并且其本身检查暂时保护密钥 CPi 的产生以及敏感信息 ISj 的加密或解密. 较少发生的情况是，保密模块和有权利的管理机构的终端协同工作，或者在开始使用保密模块之前以便对其进行初始化，或在保密模块的有效期内使有权利的管理机构检查保密模块或修改它的功能或其中包含的数据；在后一种情况下，暂时保护密钥 CPi 的产生和/或敏感信息 ISj 的加密或解密可以在该

管理机构的控制下而不再是在保密模块的控制下可靠地进行.

图 4 是在敏感信息被存储在保密模块的非易失存储器 10 中之前对于任何敏感信息 ISj 进行初始加密处理的流程图. 一个典型的例子是当所述处理从保密模块的外部由想要在其中存储敏感信息 ISj 的管理机构启动时. 首先, 在步 41 , 保密模块在工作存储器 14 中存储从外部收到的新的敏感信息 ISj , 接着, 在步 42 , 保密模块或者有权利的管理机构决定是使用新的暂时保护密钥 CPi 或使用原有的密钥计算敏感信息 ISj . 如果响应是否定的, 则保密模块的处理装置 9 将选择 (步 43) 已存在于非易失存储器 10 中的一个暂时保护密钥, 并将其传递到 (步 44) 易失的工作存储器 14 中. 在图 3 的例子中, 这是号数为 Ni 的密钥 CPi . 关于密钥值, 保密模块选择具有最高下标的一个: 在本例中是下标 (ai+1),但是如果该密钥一直未被更新过, 则将是下标 1 . 相反, 如果在步 42 确定必须由保密模块产生一个新的暂时保护密钥, 则在步 45 在工作存储器 14 中产生所述密钥, 并把产生的密钥保留在 (步 46) 非易失存储器中以备后用.

在步 47 , 保密模块利用密钥 CPi 计算信息 ISj , 从而获得结果 $\overline{ISj}_{(ai+1)}$. 在步 48 , 保密模块把这个结果存储在专用于这种敏感信息的非易失存储器区域中. 自然, 如图 3 所示, 和敏感信息 $\overline{ISj}_{(ai+1)}$ 一道, 保密模块存储所用密钥的号数 Ni 和更新下标 (ai+1) .

图 5 是用于解密敏感信息 $\overline{ISj}$ 以便在保密模块的内部进行处理作业时的流程图. 在步 51 , 发出使用敏感信息 ISj 的请求, 例如在启动数据处理装置 1 时, 从而在步 52 保密模块把处于其加密形式 $\overline{ISj}_{(ai+1)}$ 的敏感信息和相应的暂时保护密钥 CPi (以合适的 ai+1 的型式) 从其非易失存储器 10 中传递到其工作存储器 14 . 然后使用密钥解密敏感信息 (步 53) , 从而获得解密的敏感信息 ISj . 在步 54 , 保密模块在要被进行的处理中使用解密的敏感信息 ISj . 注意, 在要被进行的处理中使用之后, 解密的敏感信息 ISj 将消失并且最终不再存在于保密模块中. 在本例中, 这通过易失存储器的特性实现, 使得在与信息处理装置 1 的通信结束而进入省电状态时其所含的信息消失.

图 6 是任何暂时保护密钥 CPi 的定期刷新处理 (更新) 的流程图. 其

主要优点在于，用这种方式产生密钥内容的改变，使得难于通过解密密钥实现欺骗的企图；此外，通过进一步加密相关的敏感信息，这个刷新的密钥将以其加密的形式刷新该信息，使得从信息的加密的形式解密敏感信息的内容更加困难．显然，黑客可以观测到保密模块的端子之间的电信号，特别是非易失存储器和工作存储器 14 之间转移数据的期间，因为实际上信号总是受保密模块进行的处理的性质的影响．只要黑客存储大量的这种观测并进行统计分析，便有可能重构有关的敏感信息．

图 6 的处理或者以预定的或甚至随机的周期在保密模块进行刷新其暂时保护密钥时启动，或者在信息处理装置 1 向保密模块发出合适的信息或指令时启动，虽然在后一种情况下，除去在数据处理装置 1 是有权利的管理机构的特殊情况之外，处理的执行在保密模块的控制下进行．刷新最好以取决于正在讨论的敏感信息的类型的周期进行：因而，对于例如机密的用户代码或 PIN（ Personal Identification Number 个人识别码）类型的敏感信息，其速率将较高，因为其通常含有少量的指针并且使用频繁，和加密密钥或特征标记相比更容易舞弊．保密模块可以在其非易失存储器 10 中存储关于每项敏感信息的刷新速率的指示，这是非常有利的．例如，可以在有关的敏感信息已被使用一个预定的次数时提供这一刷新速率．

在开始步 61 中，保密模块查看图 2 的表，确定对于其保护的所有敏感信息，其要刷新的暂时保护密钥 CPi 是否是最高的更新下标．其实应该记住，对于每个密钥，最好只保留两个连续的型式，密钥刷新时预先假定删除老的型式，以便在原位写入更新的一个．然而，这种方法中只有当前没有要求使用老的型式解密的存储的敏感信息时，所述的删除才是可能的；否则，解密将是不可能的．

如果在步 61 中设置的条件不满足，则保密模块将更新有关敏感信息的加密形式．首先，在步 62，其把该敏感信息（在这种情况下，只有敏感信息项 $\overline{IS(j-1)_{ai}}$ ）连同暂时保护密钥 CPi 的相应的值 CPi_{ai} 和该密钥的最近的值 $CPi_{(ai+1)}$ 转移到工作存储器 14 中．在步 63，其利用密钥 CPi_{ai} 解密敏感信息 $\overline{IS(j-1)_{ai}}$，然后，在步 64，在非易失存储器 10 的一个缓冲区内保留敏感信息 $\overline{IS(j-1)_{ai}}$（即以其加密的形式），以便阻止在随后 IS（ j-1 ）

的再次加密被中断的情况下被丢失. 在步 65 期间，保密模块利用暂时保护密钥 CPi 的最新近的值 CPi（ai+1）再次加密恢复的敏感信息 IS（ j-1 ），从而获得敏感信息 IS（ j-1 ）的加密形式的最新近的型式 $\overline{IS(j-1)}_{(ai+1)}$. 最后，在步 66，保密模块用最新近的值 $\overline{IS(j-1)}_{(ai+1)}$ 代替在非易失存储器 10 中的最老值 $\overline{IS(j-1)}_{ai}$，并通过使更新下标（ ai ）增加一个单位对其更新从而获得（ ai+1 ）：这种情况由图 8 表中第三和第四栏的黑体字符所示.

在此步之后，或者步 61 的条件已被满足，则在步 67，保密模块将以新的更新下标（ ai+2 ）在工作存储器 14 中产生暂时保护密钥 CPi 的新值 CPi（ai+2）. 如前所述，在最佳实施例中，这个新值是随机数或和随机数有关. 最后，在步 68，保密模块在其图 2 的表中在非易失存储器 10 中用最新近的一个 CPi（ai+2）代替暂时保护密钥 CPi 的最老的值 CPi_{ai}，并使更新下标（ ai ）增加 2 个单位对其更新从而获得（ ai+2 ）：这种情况在图 7 中表的第三和第四栏中用黑体字符表示.

图 9 是对于任何敏感信息进行定期刷新处理的流程图. 一般地说，这种处理接着图 6 的密钥刷新处理，并特别涉及和用这种方式刷新的密钥有关的敏感信息；然而，作为一种代替方案，它可以在稍后的任何时刻被执行. 类似于图 6 的处理，或者在保密模块被设置以预定的或随机的速率开始刷新其敏感信息时，或者在数据处理装置为此向保密模块发送合适的信息或指令时，该处理被启动，虽然在后一种情况下，除去数据处理装置 1 是有权利的管理机构的处理装置之外，处理的执行只能在保密模块的唯一控制下进行.

在步 91，发出敏感信息刷新请求. 在步 92，保密模块将有关的敏感信息和其暂时保护密钥传送到工作存储器 14 中：在本例中，其涉及敏感信息 $\overline{IS(j-1)}_{(ai+1)}$ 和 $\overline{ISj}_{(ai+1)}$，以及密钥 CPi（ai+1）和 CPi（ai+2）. 在步 93，保密模块利用密钥 CPi（ai+1）解密这敏感信息，然后，在步 94，利用密钥 CPi（ai+2）再加密这样获得的敏感信息 IS（ j-1 ）和 ISj. 在步 95，存储再加密的敏感信息 $\overline{IS(j-1)}_{(ai+2)}$ 和 $\overline{ISj}_{(ai+2)}$ 在非易失存储器的前述的缓冲区中. 最后，在步 96，在非易失存储器的专用区中存储该数据代替敏感信息

$\overline{IS(j-1)}_{(ai+1)}$ 和 $\overline{ISj}_{(ai+1)}$，并使更新下标（ ai+1 ）增加一个单位对其更新得到（ ai+2 ）：这种情况在图 8 的表中第 5 和第 6 栏用黑体字符表示。

关于上述的各个步骤，步骤链可以被保密模块的信息处理装置 9 暂时地中断，以便执行和本发明的方法无关的但在给定时刻被认为是优先的其它任务。在这种情况下，在这些任务处理结束时将恢复本程序。此外，保密模块处理暂时保护密钥和敏感信息的顺序可以根据各种方案而改变。例如，图 6 的处理确保密钥 CPi 的完全刷新和其它密钥的刷新无关；在另一种方案中，保密模块同时刷新几个密钥，而图 6 对每个密钥为特定的步骤并和对其它密钥为特定的步骤相邻或交错。

关于在解密的敏感信息为一个给定的处理任务被使用之后使该信息取消的方式，下面的例子使用易失存储器(在本例中为工作存储器 14)在和信息处理装置 1 结束通信后加电时引起信息丢失的特性。作为一种替代，如果用于暂时存储敏感信息的存储器是非易失存储器，则需要使用由保密模块的微处理器 9 执行的特定指令从存储器中擦除所述信息。这里在一些地方所用的“暂时存储解密的敏感信息，使得其在使用之后从保密模块中消失”这一表述旨在更明确地包括所述两种执行的形式。

在使用一个非对称的公共密钥算法的上述的本发明的变型情况下，和这类似的算法一般接收 512 位格式的数据，即，远远大于敏感信息的一般格式（ 64 位）。其优点在于，在由这算法进行公共加密之前进行信息的多个敏感项的分组或组合，以便达到总共 512 位的格式。

在上述的例子中，保密模块 8 一般以和信息处理装置 1 相连的方式操作。作为一种替代，保密模块具有为本身提供电能的装置，并以独立的方式，即不和信息处理装置相连，执行上述的用于存储和使用敏感信息的处理，或至少执行其中一些步骤。

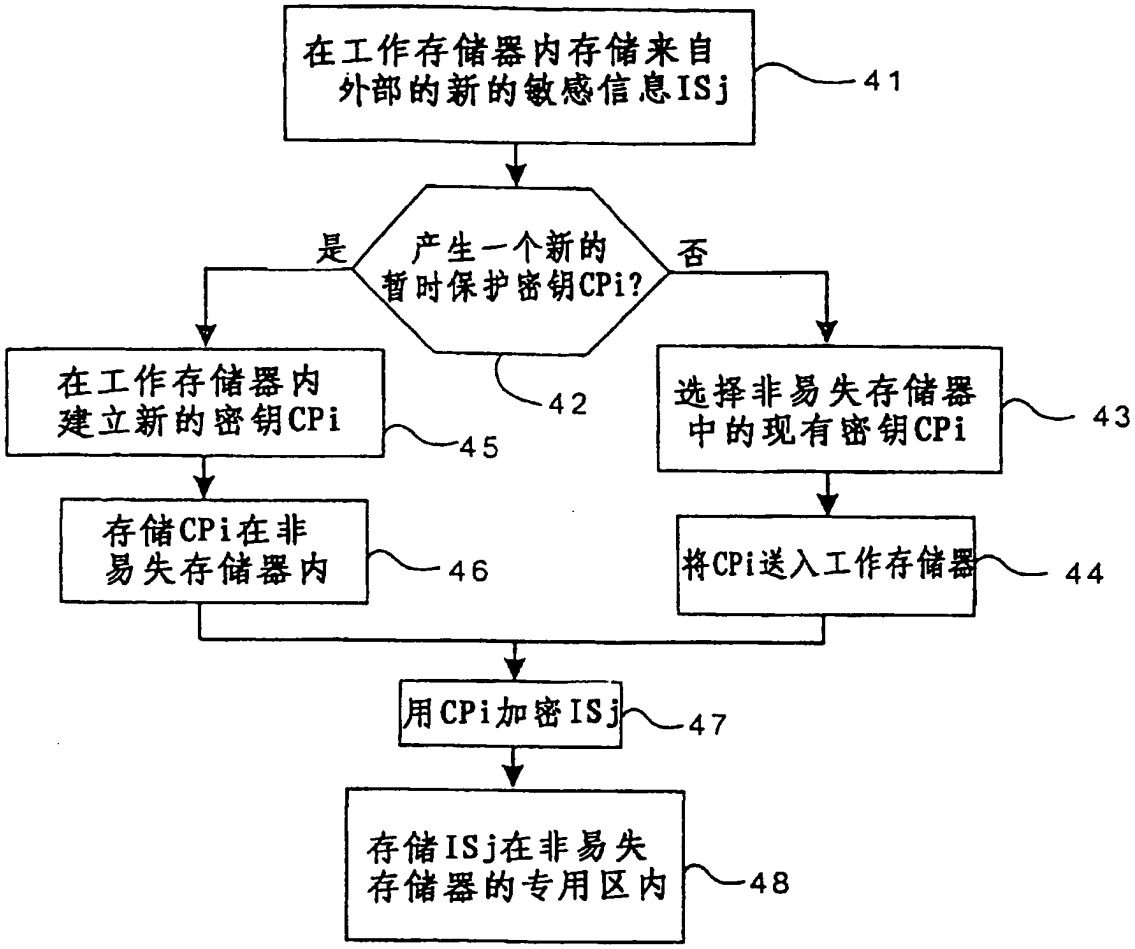

在工作存储器内存储来自外部的新的敏感信息ISj
41
产生一个新的暂时保护密钥CPi?
是
否
42
在工作存储器内建立新的密钥CPi
45
选择非易失存储器中的现有密钥CPi
43
存储CPi在非易失存储器内
46
将CPi送入工作存储器
44
用CPi加密ISj
47
存储ISj在非易失存储器的专用区内
48

图 4

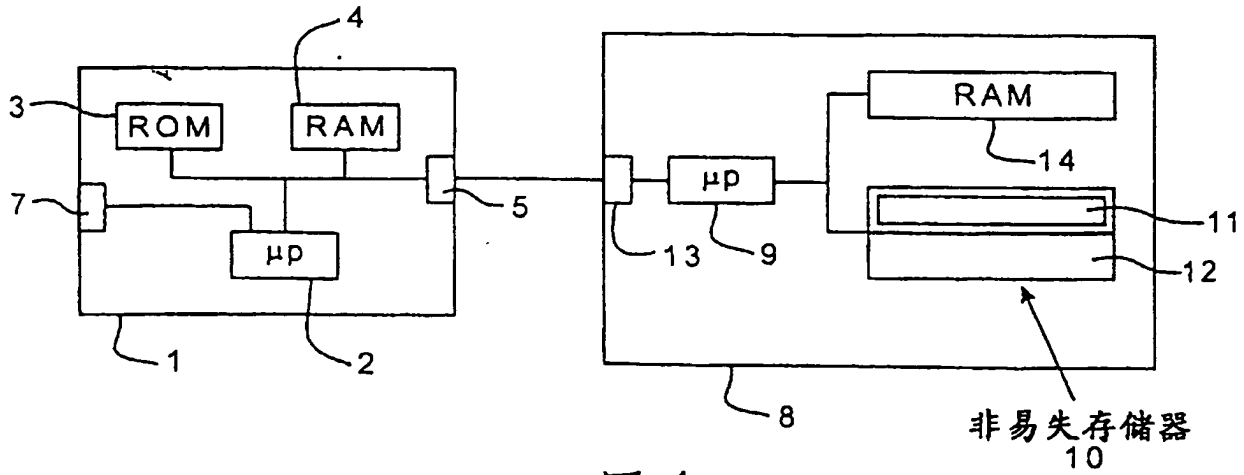

4
3
ROM
RAM
7
μp
5
1
2
μp
RAM
14
13
9
11
12
8
非易失存储器
10

图 1

暂时保护密钥	密钥号	更新下标	存储的密钥值
CP1	N1	a1 --- a1+1	$CP1_{a1}$ --- $CP1_{(a1+1)}$
. . . .	. . . .	. . . .	. . . .
CPi	Ni	ai --- ai+1	CPi_{ai} --- $CPi_{(ai+1)}$
. . . .	. . . .	. . . .	. . . .
CPn	Nn	an --- an+1	CPn_{an} --- $CPn_{(an+1)}$

图2

参考的敏感信息	相关密钥号	当前密钥下标	敏感信息的存储型式
IS1	N1	a1+1	$\overline{IS1}_{(a1+1)}$
IS2	N1	a1+1	$\overline{IS1}_{(a1+1)}$
. . . .	. . . .	. . . .	. . . .
IS(j-1)	Ni	ai	$\overline{IS(j-1)}_{ai}$
ISj	Ni	ai+1	$\overline{ISj}_{(ai+1)}$
. . . .	. . . .	. . . .	. . . .
ISm	Nn	an+1	$\overline{ISm}_{(an+1)}$

图3

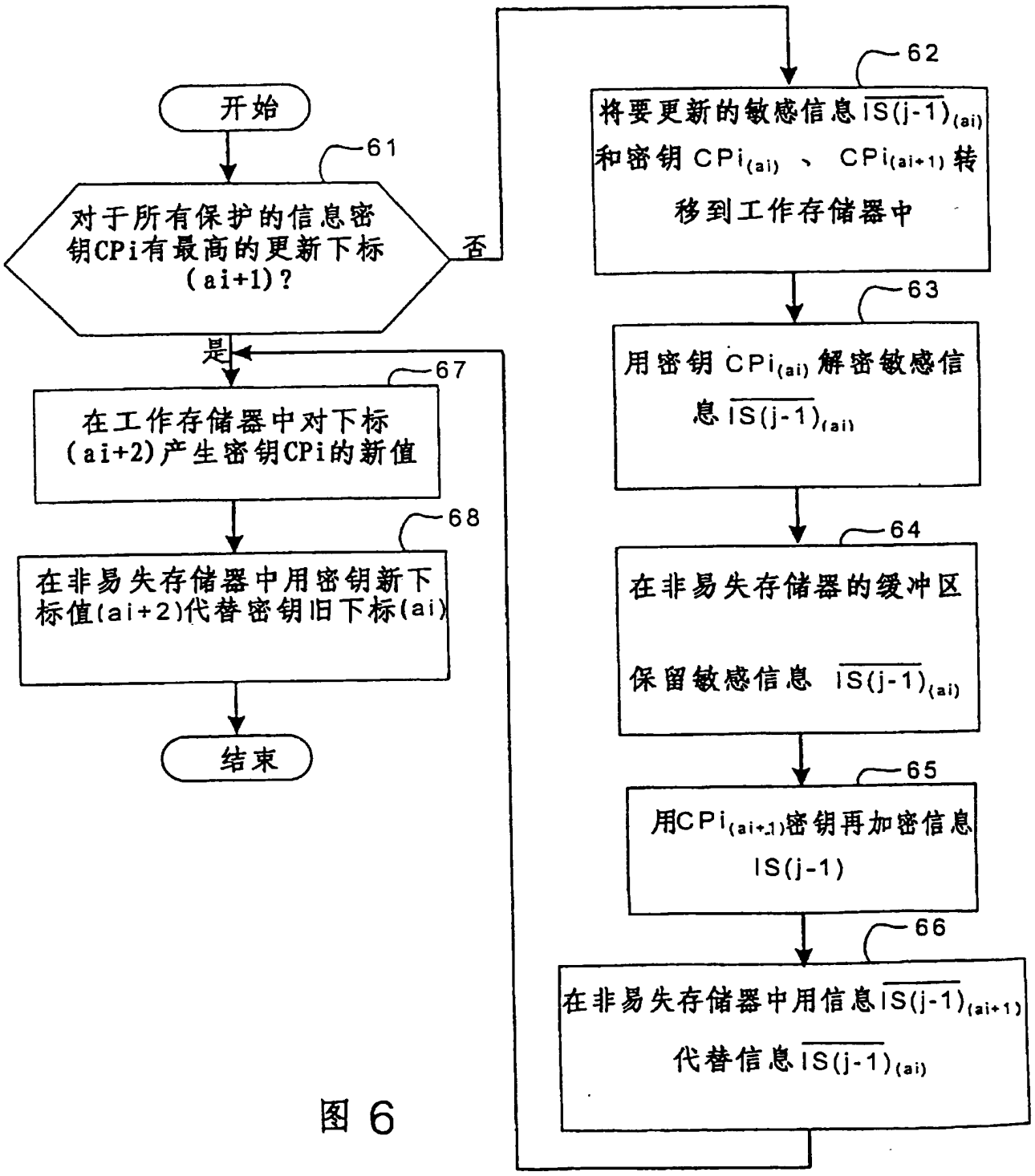

开始
61
对于所有保护的信息密钥CPi有最高的更新下标(ai+1)?
否
是
62
将要更新的敏感信息$\overline{IS(j-1)}_{(ai)}$和密钥$CPi_{(ai)}$、$CPi_{(ai+1)}$转移到工作存储器中
63
用密钥$CPi_{(ai)}$解密敏感信息$\overline{IS(j-1)}_{(ai)}$
64
在非易失存储器的缓冲区保留敏感信息$\overline{IS(j-1)}_{(ai)}$
65
用$CPi_{(ai+1)}$密钥再加密信息IS(j-1)
66
在非易失存储器中用信息$\overline{IS(j-1)}_{(ai+1)}$代替信息$\overline{IS(j-1)}_{(ai)}$
67
在工作存储器中对下标(ai+2)产生密钥CPi的新值
68
在非易失存储器中用密钥新下标值(ai+2)代替密钥旧下标(ai)
结束

图 6

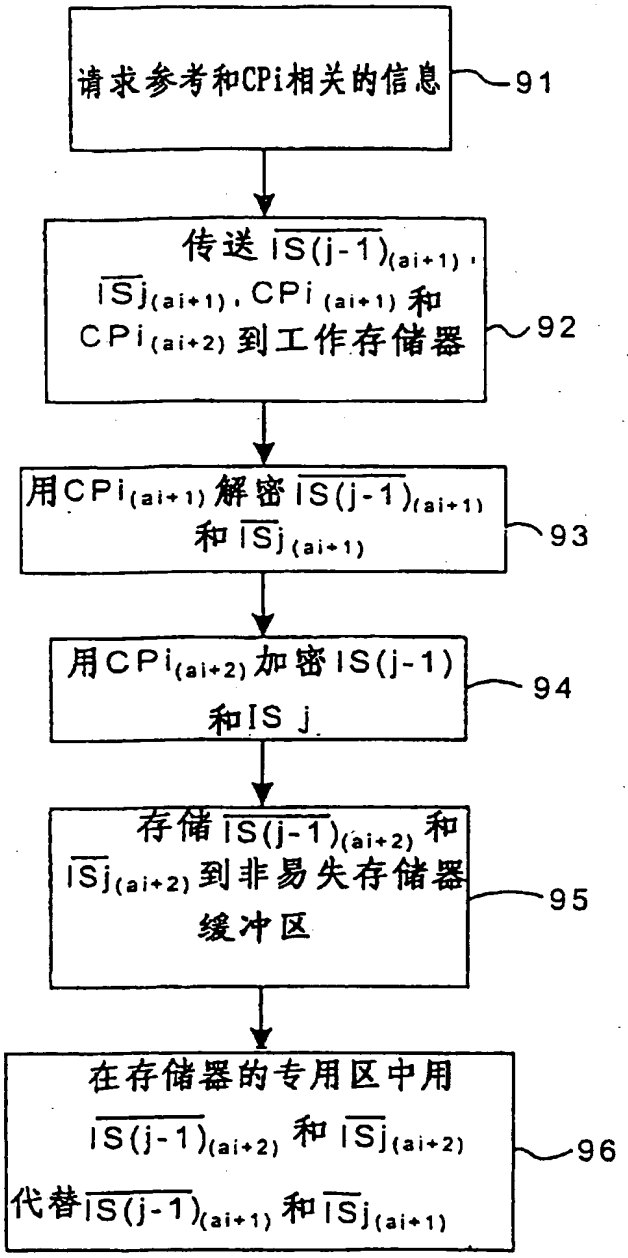

请求参考和CPi相关的信息
91
传送 $\overline{IS(j-1)}_{(ai+1)}$, $\overline{ISj}_{(ai+1)}$, $CPi_{(ai+1)}$ 和 $CPi_{(ai+2)}$ 到工作存储器
92
用 $CPi_{(ai+1)}$ 解密 $\overline{IS(j-1)}_{(ai+1)}$ 和 $\overline{ISj}_{(ai+1)}$
93
用 $CPi_{(ai+2)}$ 加密 IS(j-1) 和 IS j
94
存储 $\overline{IS(j-1)}_{(ai+2)}$ 和 $\overline{ISj}_{(ai+2)}$ 到非易失存储器缓冲区
95
在存储器的专用区中用 $\overline{IS(j-1)}_{(ai+2)}$ 和 $\overline{ISj}_{(ai+2)}$ 代替 $\overline{IS(j-1)}_{(ai+1)}$ 和 $\overline{ISj}_{(ai+1)}$
96

图 9

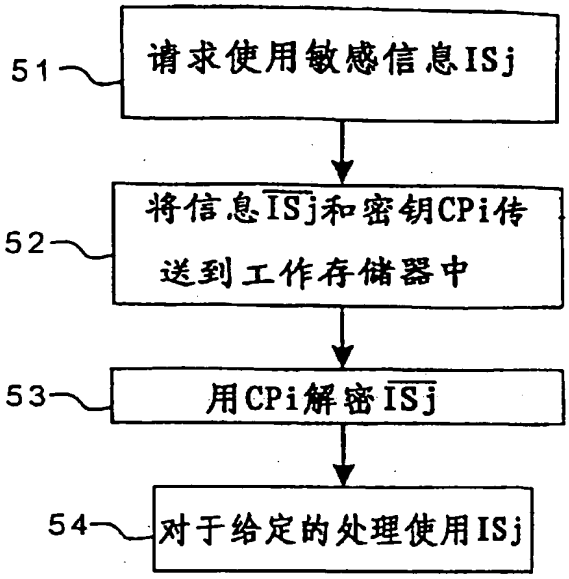

51
请求使用敏感信息ISj
52
将信息$\overline{ISj}$和密钥CPi传送到工作存储器中
53
用CPi解密$\overline{ISj}$
54
对于给定的处理使用ISj

图 5

临时保护密钥	密钥号	更新下标	存储的密钥值
CP1	N1	a1 --- a1+1	$CP1_{a1}$ --- $CP1_{(a1+1)}$
.	.	.	.
CPi	Ni	ai+2 --- ai+1	$CPi_{(ai+2)}$ --- $CPi_{(ai+1)}$
.	.	.	.
CPn	Nn	an --- an+1	CPn_{an} --- $CPn_{(an+1)}$

图 7

参考敏感信息	相关的密钥号	当前密钥下标	敏感信息存储型式	新的密钥下标	新的敏感信息存储型式
IS1	N1	a1+1	$\overline{IS1}_{(a1+1)}$		
IS2	N1	a1+1	$\overline{IS1}_{(a1+1)}$		
.	.	.	.	.	.
IS(j-1)	Ni	ai+1	$\overline{IS(j-1)}_{(ai+1)}$	ai+2	$\overline{IS(j-1)}_{(ai+2)}$
ISj	Ni	ai+1	$\overline{ISj}_{(ai+1)}$	ai+2	$\overline{ISj}_{(ai+2)}$
.	.	.	.	.	.
ISm	Nn	an+1	$\overline{ISm}_{(an+1)}$		

 图8